Chapter I9: HIPAA and Confidentiality

19.1 Purpose of Chapter 19

19.2 Definitions

19.3 HIPAA Determinations by DHSS

19.4 HIPAA Policies and Procedures

19.5 Accounting for Disclosures

19.6 (reserved)

19.7 Event Report

19.7CE Attachment CE: Event Report form for DHSS Covered Entities

19.7O Attachment O: Event Report form for other DHSS entities

19.7 Event Report- Attachment 1 (name and contact information of individual(s)/consumer(s))

19.8 Breach Notification

19.8A Attachment A: Event Review/Risk Assessment Form

19.8B Attachment B: Action Report Form

19.8C Breach Notification Flowchart

SUBJECT: HIPAA AND CONFIDENTIALITY Introduction: Purpose of Chapter 19	*Chapter:* 19
	Section: 19.1
REFERENCES:	*Page:* 1 of 2
	Adopted: 7/23/10

INTRODUCTION: PURPOSE OF CHAPTER 19

I. PURPOSE:

To address the impact of the Health Insurance Portability Act of 1996, its regulations, and other federal and Missouri law with regard to privacy and confidentiality of information about individuals or consumers that is obtained, accessed, used, maintained, or disclosed by or on behalf of the Department of Health and Senior Services ("DHSS").

II. SCOPE:

Departmentwide.

III. POLICY:

A. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its regulations provide individuals with specific rights with regard to information about them, including privacy of their information, and impose specific obligations on regulated entities and their contractors.

B. Other federal laws require privacy and confidentiality of information and impose specific obligations on regulated entities.

C. Numerous Missouri laws provide privacy and confidentiality to individuals regarding information about them and impose specific obligations on DHSS and other users of such information.

D. It is the intent that all DHSS policies and procedures are in accordance with applicable federal and state law, including HIPAA and its regulations and the specific applicable confidentiality laws of Missouri. If they should be found to be in conflict with existing or future laws or regulations, such laws or regulations shall supersede and prevail.

E. All DHSS employees and workforce are expected to comply with all applicable Departmental policies and procedures.

SUBJECT: HIPAA AND CONFIDENTIALITY Introduction: Purpose of Chapter 19	*Chapter:* 19
	Section: 19.1
REFERENCES:	*Page:* 2 of 2
	Adopted: 7/23/10

Prepared By:

Approved By:

_____

Chair, DHSS HIPAA Committee

_____

Deputy Department Director

SUBJECT: HIPAA AND CONFIDENTIALITY DEFINITIONS	*Chapter:* 19
	Section: 19.2
REFERENCES:	*Page:* 1 of 10
	Adopted: 7/23/10

DEFINITIONS

I. PURPOSE:

The purpose of this policy is to define terms relevant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and section 407.1500, RSMo.

II. SCOPE:

Departmentwide.

III. HIPAA DEFINITIONS:

A. The HIPAA Privacy Rule addresses protected health information in any form or format and provides the following definitions:

1. *Access is* the inspecting or obtaining a copy of protected health information.
2. *Business Associate* is a person who is not part of a covered entity's workforce who acts on behalf of the covered entity to perform a function involving the use or disclosure of protected health information.
3. *Covered entity* is a health plan; a health care clearinghouse; or a health care provider who transmits any health information in electronic form in connection with a transaction as per 45 CFR 160.103.
4. *Covered function* is a function which makes the entity a health plan, health care provider, or health care clearinghouse.
5. *Data aggregation* is, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

6. *De-identified* information is information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual; therefore de-identified information is not individually identifiable health information and not protected health information. In order to be considered de-identified, the record must have the following identifiers of the individual or of relatives, employers, or household members of the individual, removed (A) names; (B) all geographic subdivisions smaller than state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of zip code if the geographic unit combining all zip codes with the same three initial digits contains more than 20,000 or the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000; (C) all elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; (D) telephone numbers; (E) fax numbers; (F) email addresses; (G) Social Security numbers; (H) medical record numbers (I) health plan beneficiary numbers; (J) account numbers; (K) certificate/license numbers; (L) VIN or serial numbers, including license plate numbers; (M) device identifiers and serial numbers; (N) URLs; (O) IP address numbers; (P) biometric identifiers, including finger and voice prints; (Q) full face photographic images and any comparable images; and (R) any other unique identifying number, characteristic, or code. A second method to de-identify information requires an expert to document and be able to testify that in his professional opinion the expert has de-identified the information using generally accepted statistical and scientific principles and methods for rending information not individually identifiable and that the risk is very small that the information can be used alone or in combination with reasonably available information to identify an individual. In addition, the covered entity cannot have actual knowledge that the information could be used alone or in combination to identify the individual.

7. *Designated record set* is the **group of records** about an individual that is maintained by or for the covered entity that is the medical and billing records maintained by a provider; enrollment, payment, claims adjustment, and case and medical management record systems maintained by a health plan; **or used**

in whole or in part by or for the covered entity to make decisions about individuals- with "record" meaning **any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.**

8. *Disclosure* is the release, transfer, provision of, access to, or divulging in any other manner of information outside of the entity holding the information.

9. *Health care* is care, services, or supplies related to the health of an individual, including but not limited to preventative, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body.

10. *Health care operations* is **any of the following activities of the covered entity** to the extent that the activities are related to covered functions: (1) conducting quality assessment and improvement activities…, (2) reviewing the competence and qualifications of health care professionals… and non-health care professionals..., (3) underwriting…, (4) conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs, (5) business planning and development…, (6) business management and general administrative activities of the entity, including HIPAA and other legal compliance, customer service, resolution of internal grievances, the sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity…

11. *Health care provider* is a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other **person or organization who furnishes, bills, or is paid for health care in the normal course of business**.

12. *Health information* is any information, **whether oral or recorded in any form** or medium, that is **created or received by a covered entity, public health authority, employer, life insurer, school, or university** and relates to the past, present, or future physical or mental health or condition of an

individual or the past, present, or future payment for the provision of health care to an individual.

13. *Health oversight agency* is an agency or authority of the United States, a state, a territory, a political subdivision of a State… or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine the eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

14. *Hybrid entity* is a single legal entity whose business activities include both covered and non-covered functions and designates its components performing covered functions.

15. *Indirect treatment relationship* is a relationship between an individual and a provider in which the provider delivers health care to the individual based on the orders of another provider and the provider typically provides the services or products, or reports the diagnosis or results associated with the health care, directly to another provider, who provides the services or products or reports to the individual (e.g. the state public health laboratory).

16. *Individual* is the person who is the subject of protected health information and who has rights under HIPAA and its regulations.

17. *Individually identifiable health information* is information that is the subset of health information, including demographic information collected from an individual that is **created or received by a covered entity or employer** and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to an individual and identifies, or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

18. *Limited data set* is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

    a) Names;

b) Postal address information, other than town or city, state, and zip code;

c) Telephone numbers;

d) Fax numbers;

e) E-mail addresses;

f) Social Security numbers;

g) Medical record numbers;

h) Health plan beneficiary numbers;

i) Account numbers;

j) Certificate/license numbers;

k) Vehicle identifiers and serial numbers, including license plate numbers;

l) Device identifiers and serial numbers;

m) Web universal locators (URLs);

n) Internet Protocol (IP) address numbers;

o) Biometric identifiers, including finger and voice prints; and

p) Full face photographic images and any comparable images.

19. *Payment* is the activities by a health plan to obtain premiums or provide coverage or benefits under the plan or by a health plan or provider to obtain or provide reimbursement…

20. *Personal representative* is a person with legal authority to act on the individual's behalf with regard to medical records as per state law.

21. *Protected health information* is individually identifiable health information that is **transmitted or maintained electronically or transmitted or maintained in any other form or medium**, except for information protected by FERPA or records held by a covered entity in its employment capacity.

22. *Public health authority* is an agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its

contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

23. *Treatment* is the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

24. *Use* is the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

25. *Workforce* means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

B. The HIPAA Security Rule addresses protected health information in electronic form or format and provides the following definitions:

1. *Access* is the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

2. *Authentication* is the corroboration that a person is the one claimed.

3. *Availability* is the fact that data or information is accessible and useable upon demand by an authorized person.

4. *Confidentiality* is the fact that data or information is not made available or disclosed to unauthorized persons or processes.

5. *Electronic protected health information* is protected health information that is transmitted or maintained electronically.

6. *Encryption* is the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

7. *Information system* is the interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

8. *Integrity* is the fact that data or information has not been altered or destroyed in an unauthorized manner.

9. *Password* is confidential authentication information composed of a string of characters.

10. *Security* is all of the administrative, physical, and technical safeguards in an information system:

    a) *Administrative safeguards* are administrative actions, policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information;

    b) *Physical safeguards* are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion; and

    c) *Technical safeguards* are the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

11. *Security incident* is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

C. The HIPAA Breach Notification Rule imposes a requirement of notification to an individual of a breach of unsecured protected health information and provides the following definitions:

1. *Breach* is the acquisition, access, use, or disclosure of protected health information in a manner not permitted by the Privacy Rule which compromises the security or privacy of the protected health information.

   Breach excludes:

   a) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or

use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by the HIPAA Privacy Rule;

b) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted by the HIPAA Privacy Rule;

c) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information;

d) A use or disclosure that does not include:

(1) Date of birth;

(2) Zip codes; and

(3) Any of the identifiers that must be excluded to create a limited data set as per 45 CFR 164.514(e)(2).

2. *Compromise* is posing a significant risk of financial, reputational, or other harm to the individual.

3. *Unsecured protected health information* is protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS- HHS has specified that electronic protected health information is unsecure unless it is encrypted as per specific standards provided under the rule and that protected health information in paper format is unsecure unless it is properly destroyed.

IV. MISSOURI DEFINITIONS:

SUBJECT: HIPAA AND CONFIDENTIALITY DEFINITIONS	*Chapter:* 19
	Section: 19.2
REFERENCES:	*Page:* 9 of 10
	Adopted: 7/23/10

A. Section 407.1500, RSMo, addresses personal information in electronic format or medium, imposes a requirement of notification to an individual of a breach, and provides the following definitions:

1. *Breach of security*, or *breach*, is unauthorized access to and unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information.

    a) Good faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person is not a breach of security, provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.

2. *Consumer* is an individual who is a resident of this state.

3. *Encryption* is the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.

4. *Health insurance information* is an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual.

5. *Owns or licenses* includes, but is not limited to, personal information that a business retains as part of the internal customer account of the individual or for the purpose of using the information in transactions with the person to whom to information relates.

6. *Medical information* is any information regarding the individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

7. *Person* is any individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, government, governmental subdivision, governmental agency, governmental instrumentality, public corporation, or any other legal or commercial entity.

8. *Personal information* is an individual's first name or first initial and last name in combination with any one or more of the following data elements that relate

to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or date elements are unreadable or unusable:

a) Social Security number;

b) Driver's license number or other unique identification number created or collected by a government body;

c) Financial account number, credit account number, or debit account number in combination with any required security code, access code, or password that would permit access to an individual's financial account;

d) Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account;

e) Medical information; or

f) Health insurance information.

Personal information does not include information that is lawfully obtained from publicly available sources, or from federal, state, or local government records lawfully made available to the general public.

9. *Redacted* is altered or truncated such that no more than five digits of a social security number or the last four digits of a driver's license number, state identification card number, or account number is accessible as part of the personal information.

Prepared By:

Approved By:

_____

Chair, DHSS HIPAA Committee

_____

Deputy Department Director

SUBJECT: HIPAA AND CONFIDENTIALITY HIPAA DETERMINATIONS BY DHSS	*Chapter:* 19
	Section: 19.3
REFERENCES:	*Page:* 1 of 9
	Adopted: 7/23/10

HIPAA DETERMINATIONS BY DHSS

I. PURPOSE:

The purpose of this policy is to inform all Department of Health and Health Services (DHSS) workforce members and users of DHSS information of determinations made by DHSS as part of its compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its regulations.

II. SCOPE:

Departmentwide.

III. REQUIRED DETERMINATIONS

A. **STATUS DETERMINATION** (45 CFR 164.105): DHSS is a hybrid entity composed of:

1. The Division of Regulation and Licensure performs regulatory and licensing ("health oversight") functions and is **not a covered entity**.
2. The Division of Senior and Disability Services (DSDS) provides "protective services" including the coordination of care, assessment, and authorization for In-Home Services and Consumer Directed Services for "eligible adults" as defined under section 660.255, RSMo, that are covered functions of a health care provider and **is a covered entity**.
    a) Although housed in DSDS, the Central Registry Unit ("CRU") **is not a covered entity.** It serves as the intake unit for all reports of abuse, neglect and financial exploitation made to DHSS, including but not limited to reports received pursuant to:
        (1) Sections 660.255 and 565.188 (regarding any elderly or disabled adult);
        (2) Sections 660.300 and 660.305 (regarding In-Home Services clients);
        (3) Sections 208.912 and 208.915 (regarding Consumer Directed Services consumers);

(4) Sections 198.070 and 198.090 (regarding nursing home residents);

(5) Section 197.268 (regarding hospice patients);

(6) 19 CSR 30-90.050(6) (regarding adult day care clients);

(7) Section 197.435, 19 CSR 30-26.010(2)(H), and 42 CFR 484.10(f) (regarding home health agency clients); and

(8) Section 630.163 (regarding reports of abuse of vulnerable persons to be referred to the Department of Mental Health).

3. The Division of Community and Public Health performs varied functions and **is a hybrid entity:**

   a) Some portions perform non covered functions as Missouri's primary "public health" authority; and

   b) Some portions perform the covered functions of:

      (1) A health care provider by coordinating care; or

      (2) A health plan by providing health coverage (e.g. such as a payer of last resort).

4. The Director's Office provides supervision and management for all of DHSS and its units provide specialized support services for all of DHSS- when dealing with a covered entity component the Director's Office is performing health care operations:

   a) Office of Governmental Policy and Legislation;

   b) Office of General Counsel;

   c) Office of Public Information; and

   d) Office of Human Resources.

5. The Division of Administration provides fiscal, financial and general support functions for all of DHSS- when dealing with a covered entity component the Division of Administration is performing health care operations; and

6. The state Office of Administration, Information Technology Services Division assigns staff to DHSS to provide information technology support services for the HIPAA covered entity and the non-covered entity parts of DHSS. These

ITSD specialists work under an MOU between DHSS and OA/ITSD and act as workforce members of DHSS.

B. **PRIVACY OFFICER DESIGNATION** (45 CFR 164.530(a)): DHSS has designated a Privacy Officer who can be reached at 573-751-6005, at the Office of General Counsel. The privacy officer's role is to function as the official designated to coordinate development and implementation of administrative, physical, and technical safeguards for compliance with the HIPAA Privacy Rule and other confidentiality issues.

1. 45 CFR 164.530(a) requires DHSS to designate a contact person to receive complaints regarding violations of the Privacy Rule and for individuals to contact for further information about the Notice of Privacy Practices. DHSS has designated the Privacy Officer to serve this role. (See Notice of Privacy Practices)
2. 45 CFR 164.530(b) requires DHSS to provide and document training about the Privacy Rule for its workforce. (See Policies 9.1, 9.2, 11.6, 11.6A, 18.3, and 18.3A)
3. 45 CFR 164.530(c) requires DHSS to adopt administrative, physical, and technical safeguards to protect the privacy of protected health information by:
   a) Reasonably safeguarding protected health information from uses and disclosures in violation of the Privacy Rule. (See Policies 5.9, 5.9A, 9.1, 9.2, 11.6, 11.6A, 11.11); and
   b) Reasonably safeguarding protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure under the Privacy Rule but that are unnecessary. (See Policies 5.9, 5.9A, 11.6 and 11.6A)
4. 45 CFR 164.530(d) requires DHSS to provide a process for individuals to make complaints concerning its policies or its compliance under the Privacy Rule. (See Notice of Privacy Practices)
5. 45 CFR 164.530(e) requires DHSS to have and apply appropriate sanctions for failure to comply with the privacy policies and procedures or the Privacy Rule. (See Policy 10.4, 11.6, 11.6A, 13.1, and 13.2)

6. 45 CFR 164.530(f) requires DHSS to mitigate to the extent practicable any harmful effect known by DHSS resulting from a use or disclosure in violation of its policies or the Privacy Rule. (See Policy 19.8)
7. 45 CFR 164.530(g) prohibits retaliation by DHSS against anyone for filing of a complaint or acting on the rights granted by the Privacy Rule. (See Notice of Privacy Practices and Policies 12.5 and 19.7)
8. 45 CFR 164.530(h) prohibits DHSS from requiring individuals to waive the right to file a complaint provided under 45 CFR 160.306. (See Policy 19.7)
9. 45 CFR 164.530(j) requires DHSS to implement policies and procedures for compliance with the Privacy Rule and to update as needed to comply with the law. (See Policy 19.4)
10. 45 CFR 164.530(j) requires that the above documentation be maintained for six (6) years. (See Policy 19.4)

C. **SECURITY OFFICER DESIGNATION** (45 CFR 164.308(a) (2): DHSS has designated a Security Officer who can be reached at 800-347-0887, 573-751-6388 or at Support@dhss.mo.gov. The security officer's role is to function as the official designated to coordinate development and implementation of administrative, physical, and technical safeguards for compliance with the HIPAA Security Rule.

1. 45 CFR 164.306 requires DHSS to:
   a) Ensure confidentiality, integrity, and availability of all electronic protected health information it creates, receives, maintains, or transmits (See Policy 24.2);
   b) Protect against reasonably anticipated threats or hazards (See Policy 24.2);
   c) Protect against reasonably anticipated uses or disclosures in violation of the Privacy Rule (See Policies 11.6, 11.6A, and 24.2);
   d) Ensure compliance by workforce (See Policies 11.6, 11.6A, 24.2 and 24.3); and
   e) Adopt reasonable policies based upon:
      (1) DHSS' size, complexity and capability;

(2) DHSS' technical infrastructure, hardware, and software capabilities;

(3) The costs of security measures; and

(4) The probability and criticality of potential risks to electronic protected health information.

2. 45 CFR 164.308(a)(1) requires an Information Security Management Process with policies and procedures to prevent, detect, contain and correct security violations (See Administrative Policy Manual, Chapter 24 generally), including:

   a) Performance of a risk analysis;

   b) Risk management;

   c) Sanction policy; and

   d) Information system activity review.

3. 45 CFR 164.308(a)(3) requires workforce security measures to ensure appropriate access and to prevent inappropriate access, the following must be considered and implemented, or if not implemented an explanation documented, including:

   a) Authorization and supervision (See ASAP process and Policies 24.2 and 24.3);

   b) Workforce clearance procedure (See ASAP process and Policies 24.2 and 24.3); and

   c) Termination procedures (See ASAP process and Policies 24.2 and 24.3).

4. 45 CFR 164.308(a)(4) requires information access management policies and procedures to ensure access is granted in compliance with the Privacy Rule, or if not implemented an explanation documented, including:

   a) Access authorization (See ASAP process and Policies 24.2 and 24.3); and

   b) Access establishment and modification (See ASAP process and Policies 24.2 and 24.3).

5. 45 CFR 164.308(a)(5) requires a security awareness training program for all employees (including management), or if not implemented an explanation documented, including:

   a) Periodic security reminders (See: http://10.33.34.5/TipsTricks/Security/State_Employee_Computer_Security_Tips.pdf);

   b) Protection from malicious software (See Policy 24.7.IV.A.8);

   c) Log-in monitoring (See Policy 24.7.IV.D.8); and

   d) Password management (See: http://10.33.34.5/TipsTricks/Active_Directory/Passwords.htm and Policy 24.2).

6. 45 CFR 164.308(a)(6) requires security incident policies and procedures to identify and respond to suspected or known security incidents, mitigate their harmful effects, and document their outcomes (See Policy 24.7).

7. 45 CFR 164.308(a)(7) requires a contingency plan with policies and procedures for data backup; disaster recovery; emergency plan operations; testing and revision procedures; and applications and data criticality analysis (See Policies 16.1, 16.2, 16.3, 16.8 and 16.9).

8. 45 CFR 164.308(a) (8) requires a periodic technical and nontechnical evaluation in response to environmental or operational changes to establish whether DHSS policies and procedures meet the Security Rule requirements.

9. 45 CFR 164.308(b) requires Business Associate provisions for all DHSS covered entity contracts when the contractor will have any access to, use, maintain, create, or transmit protected health information on behalf of DHSS.

10. 45 CFR 164.310(a) requires facility access controls to limit physical access to electronic protected health information and to ensure properly authorized access (See Policy 11.27).

11. 45 CFR 164.310(b) requires workstation use policies and procedures (See Policy 24.5).

12. 45 CFR 164.310(c) requires physical security measures to restrict access to workstations (See Policy 11.27).

13. 45 CFR 164.310(d) requires:

a) Device and media controls regarding disposal and re-use of electronic media (See DHSS surplus process at: http://10.33.34.5/Processes_Procedures/surplussing_equipment.htm), and

b) Implementation of a record system to record the movement of hardware and electronic media and responsible persons and data backup and storage of electronic protected health information before movement of equipment or documentation of an explanation for not doing so (See DHSS surplus process at: http://10.33.34.5/Processes_Procedures/surplussing_equipment.htm).

14. 45 CFR 164.312 requires technical safeguards:

a) Access control, including:

(1) Unique user identification ("one user/one password") (See Policy 24.2 and http://10.33.34.5/TipsTricks/TipsTrickNav.htm);

(2) Emergency access procedures;

(3) Implementation of an automatic logoff and encryption/decryption (or documentation of an explanation for not doing so) (See Policy 24.2 generally: http://10.33.34.5/TipsTricks/Security/McAfee_Endpoint_Encryption.pdf for laptops).

(a) Audit controls.

(b) Integrity: Policies and procedures to protect the electronic protected health information from improper alteration or destruction.

(c) Person or entity authentication to verify that a person or entity seeking access to electronic protected health information is the one claimed.

(d) Transmission security *may* be addressed through:

- Integrity measures, or
- Encryption (See http://10.33.34.5/TipsTricks/Proofpoint/Instructions_for_ProofPoint_Mail_Encryption_UPDATED.pdf).

15. 45 CFR 164.314 requires DHSS to include specific Business Associate provisions in all contracts where a DHSS covered entity's contractor will have any access to, use, maintain, create or transmit protected health information on behalf of DHSS. DHSS' Business Associate provisions are posted on the DHSS intranet at http://dhssnet/Forms/index.html.
16. 45 CFR 164.316 requires documentation of the determinations referenced in III.C for compliance with the Security Rule to be maintained for six (6) years and updates to be made as needed.

D. **NOTICE OF PRIVACY PRACTICES** (45 CFR 165.520): DHSS adopted the Notice of Privacy Practices (NPP) posted at http://www.dhss.mo.gov/HIPAA/ that is available in paper form upon request:

1. DHSS health care providers provide a copy of the DHSS NPP upon first contact to individuals.
2. DHSS health plan components provide the DHSS NPP annually at sign up for coverage.

E. **ACKNOWLEDGEMENT FORM** (45 CFR 164.520(e)): DHSS has posted an Acknowledgement form at http://www.dhss.mo.gov/HIPAA/Forms.html.

F. **AUTHORIZATION FORM** (45 CFR 164.508): DHSS has posted an Authorization form that meets all the elements required by 45 CFR 164.508 for a HIPAA compliant Authorization at http://www.dhss.mo.gov/HIPAA/Forms.html. In order to make a disclosure to someone other than the individual, DHSS requires a properly filled out HIPAA compliant Authorization form signed by the individual or the individual's personal representative; a HIPAA compliant protective order; or the disclosure must be one addressed in 164.512 or 164.510.

G. **BUSINESS ASSOCIATE AGREEMENT** (45 CFR 164.502(e) and 164.504(e), 164.314, 164.414: DHSS has adopted a Business Associate Agreement for use in contracts by all DHSS covered entities that is posted at http://dhssnet/Forms/index.html.

H. **BREACH NOTIFICATION POLICY** (45 CFR 164.530(i) and section 47.1500, RSMo.): DHSS has provided a How to file a Health Information Privacy Complaint for use by individuals who believe their Privacy rights have been violated by the Missouri Department of Health and Senior Services at http://www.dhss.mo.gov/HIPAA/ContactUs.html.

Prepared By:

Chair, DHSS HIPAA Committee

Approved By:

Deputy Department Director

SUBJECT: HIPAA AND CONFIDENTIALITY DHSS HIPAA Policies and Procedures	*Chapter:* 19
	Section: 19.4
REFERENCES:	*Page:* 1 of 4
	Adopted: 7/23/10

HIPAA AND CONFIDENTIALITY

I. PURPOSE:

The purpose of this policy is to identify DHSS policies adopted for compliance with HIPAA and its regulations and other applicable confidentiality laws.

II. SCOPE:

Departmentwide.

III. DHSS POLICIES ADOPTED FOR COMPLIANCE WITH HIPAA:

1. Policy 5.9 *Telecommuting*
2. Policy 5.9A *Attachment - Telecommuting Agreement*
3. Policy 9.1 *Orientation*
4. Policy 9.2 *Training Requirements and Records*
5. Policy 10.4 *Disciplinary Action*
6. Policy 11.1 *Use of Department Property*
7. Policy 11.5 *Personal Visitors*
8. Policy 11.6 *Code of Conduct – Confidential Information*
9. Policy 11.6A *Confidentiality Agreement*
10. Policy 11.11 *Conflict of Interest*
11. Policy 11.11A *Attachment - Statement of No Conflict of Interest*
12. Policy 11.20 *Employee Identification Badges*
13. Policy 11.21 *Employee Identification Badge Replacement*
14. Policy 11.21 A *Attachment - Employee Identification Badge Replacement Request*

15. Policy 11.27 *Confidential Records and Information - Work Environment*
16. Policy 11.28 *Employee Privacy in the Workplace*
17. Policy 12.5 *Protection from Retaliation*
18. Policy 13.1 *Termination Types*
19. Policy 13.2 *Terminating Employment Checklist*
20. Policy 16.1 *COOP (Continuity of Operations Plan) Description*
21. Policy 16.2 *COOP Delegation of Authority*
22. Policy 16.3 *Supervisors' Participation in COOP Activities*
23. Policy 16.8 *COOP Remote Work*
24. Policy 16.9 *Work and Rest During COOP Activation*
25. Policy 18.3 *Annual Policy and Training Requirements*
26. Policy 18.3A *Attachment - Annual Policy Review Checklist*
27. Policy 19.1 *Purpose of Chapter 19: HIPAA and Confidentiality*
28. Policy 19.2 *HIPAA Definitions*
29. Policy 19.3 *HIPAA Determinations by DHSS*
30. Policy 19.4 *HIPAA Policies and Procedures*
31. Policy 19.5 *Accounting for Disclosures*
32. Policy 19.6 (reserved)
33. Policy 19.7 *Event Report*
34. Policy 19.7CE *Attachment - Event Report for DHSS Covered Entities*
35. Policy 19.7O *Attachment - Event Report for other DHSS entities*
36. Policy 19.8 *Breach Notification*
37. Policy 19.8A *Attachment - Action Report form*
38. Policy 19.8B *Attachment - Event Review/Risk Assessment*
39. Policy 19.8C *Attachment - Breach Notification Flowchart*
40. Policy 24.1 *Services and Jurisdiction*

41. Policy 24.2 *Security Policies and Rules*
42. Policy 24.3 *Access Request Rules and Processes*
43. Policy 24.4 *Software Use Policy*
44. Policy 24.5 *Information Technology Use Policy, Guidelines and Processes*
45. Policy 24.6 *Planning and Procurement and Installation Processes*
46. Policy 24.7 *Information Security Incident Reporting*
47. Policy 24.8 *Help Desk Request Process*
48. Policy 24.9 *Equipment Submission Process*
49. Policy 24.10 *Training Request Process*
50. Policy 24.12 *Department of Health and Senior Services (DHSS) Customer Service Request Committee (CSR) and Information Technology Advisory Committee (ITAC)*
51. Policy 24.12A1 *Appendix 1 - Customer Service Request (CSR) Process Flow Chart*
52. Policy 24.12A2 *Appendix 2 - ITAC Project Review and Approval Process Flow Chart*
53. Policy 24.12A3 *Appendix 3 - ITSD Customer Service Request (CSR / ITAC Project Submission Form*
54. Policy 24.12A4 *Appendix 4 - DHSS Criterion Scoresheet*
55. Policy 24.13 *Transfer, Reassignment or Surplus of Computer Equipment and Storage Media Disposition Process*
56. Policy 24.13A *Attachment - Procedure to Surplus Computer Equipment*
57. Policy 24.14 *Laptop and Portable Computer Security Policy*
58. Policy 24.14 A *Attachment - Laptop Custodian Agreement*
59. Policy 24.15 *Printer Management Policy*
60. Policy 24.16 *Computer to FTE Ratio Policy*

SUBJECT: HIPAA AND CONFIDENTIALITY DHSS HIPAA Policies and Procedures	*Chapter:* 19
	Section: 19.4
REFERENCES:	*Page:* 4 of 4
	Adopted: 7/23/10

IV. POLICY:

All employees and workforce members are expected to comply with all applicable Department policies and procedures. All supervisory staff and management are to assure that employees and workforce members are fully aware of and understand the policies and the importance of maintaining privacy and confidentiality of protected health information, personal information, and other sensitive or otherwise confidential information.

V. RECORDS RETENTION:

Copies of all applicable policies will be maintained for at least six (6) years as required by 45 CFR 164.530(j).

Prepared By:

_____

Chair, DHSS HIPAA Committee

Approved By:

_____

Deputy Department Director

SUBJECT: HIPAA AND CONFIDENTIALITY Accounting for Disclosures	*Chapter:* 19
	Section: 19.5
REFERENCES:	*Page:* 1 of 3
	Adopted: 7/23/10

ACCOUNTING FOR DISCLOSURES

I. PURPOSE:

To address what disclosures must be documented in order to provide an individual with an accounting of disclosures made by the HIPAA covered entity portions of Department of Health and Senior Services (DHSS) or their business associates.

II. SCOPE:

This policy applies specifically to those portions of DHSS that are HIPAA covered entities.

III. POLICY:

A. HIPAA's Privacy Rule provides an individual the right to request an accounting of disclosures made by DHSS' covered entities or business associates.

B. All DHSS employees and workforce are expected to comply with all applicable Departmental policies and procedures.

C. If an employee discloses protected health information for reasons listed below or if an unauthorized disclosure is inadvertently made, the employee should track such disclosure either electronically in the applicable electronic data system or by the Division's usual tracking protocol.

D. Disclosures of protected health information that should be tracked and provided upon a request for an accounting include protected health information disclosed:

1. To a public health authority;
2. To avert a serious threat to health or safety of a person or the public;
3. To the Food and Drug Administration;
4. To health oversight agencies for oversight activities authorized by law;
5. For judicial or administrative proceedings;

6. To law enforcement officials as required by law or pursuant to a court order or a court-ordered warrant, or a subpoena or summons issued by a judicial officer; a grand jury subpoena; or an administrative request, such as an administrative summons or a civil investigative demand; for purposes of identifying or locating a suspect, fugitive, material witness, or missing person; or regarding a crime victim;
7. About a victim of abuse, neglect, or domestic violence to a government authority to the extent the disclosure is required by law;
8. For some research purposes;
9. To governmental functions (e.g., national security, veteran's information);
10. As required by law; and
11. In addition, any disclosure, whether inadvertent or not, that is <u>not permitted under the Privacy Rule</u> should be logged for an accounting of disclosures and in addition reported as an Event as per Policy 19.7.

E. An individual has the right to receive an accounting of disclosures of protected health information made by DHSS in the six years prior to the date on which the accounting is requested, except for disclosures:

1. To carry out treatment, payment and health care operations as provided in 164.506;
2. To individuals of protected health information about themselves as provided in 164.502;
3. Incident to a use or disclosure otherwise permitted or required by the Privacy Rule, as provided in 164.502;
4. Pursuant to an authorization as provided in 164.508;
5. To persons involved in the individual's care or other notification purposes as provided in 164.510;
6. For national security or intelligence purposes as provided in 164.512(k)(2);
7. To correctional institutions or law enforcement officials as provided in 164.512(k)(5);
8. As part of a limited data set in accordance with 164.514(e); or

9. That occurred prior to the compliance date for DHSS (April 14, 2003).

F. Any individual who wishes to request an accounting of disclosures shall be asked to complete a "Request for Accounting of Disclosures of PHI" (Attachment 1) and submit it to the DHSS Privacy Officer. The DHSS Privacy Officer will coordinate the request with applicable Divisions.

G. The accounting shall be provided within sixty (60) days of the request and shall include a list of disclosures made by the covered entity or its business associate during the six (6) years prior to the request, unless the individual specifies a shorter time period, with:

1. the date of the disclosure;
2. the name, and address if known, of the person or entity who received the information;
3. a brief description of the information disclosed; and
4. a brief description of the purpose of the disclosure or a copy of the request.

However, but for multiple disclosures the covered entity can provide a shortened format.

H. The first accounting requested by an individual within any twelve (12) month period must be provided without charge; however, a covered entity may charge a reasonable cost based fee for any additional request within that time period provided the covered entity informs the individual of the charge and provides the individual the opportunity to withdraw or modify the request in order to avoid or reduce the fee.

Prepared By:

Chair, DHSS HIPAA Committee

Approved By:

Deputy Department Director

SUBJECT: HIPAA AND CONFIDENTIALITY Event Report	*Chapter:* 19 Section: 19.7
REFERENCES: Administrative Manual Policies: 11.6 Code of Conduct-Confidential Information; 11.11 Conflict of Interest; 19.7-CE or 19.7-O, Event Report Form; 24.2 Security Policies and Rules; and 24.7 Information Security Incident Reporting, and 42 U.S.C. 17921 of the HITECH Act; 45 CFR Parts 160 & 164; and §407.1500, RSMo	*Page:* 1 of 6 *Adopted:* 7/23/10

EVENT REPORT

I. PURPOSE:

This policy establishes the Department of Health and Senior Services (DHSS) Event Report process and identifies the procedures, roles and responsibilities needed for its implementation. The purpose is to establish a process to report any event that may involve a "breach" of "protected health information" or "personal information" to minimize the damage from breaches, to prevent their occurrence or recurrence, and to assist DHSS to promptly notify individuals whose protected health information or personal information was involved in a "breach."

II. SCOPE:

This policy applies to all DHSS workforce members, including all employees, Office of Administration Information Technology Services Division (ITSD) employees assigned to DHSS, interns, trainees, researchers, and volunteers. This policy applies to protected health information or personal information in any format or media, including but not limited to oral, written, and electronic. This policy applies to all DHSS information systems including but not limited to computers connected to DHSS local, statewide, and Internet communication networks, database storage systems, electronic records systems, imaging systems, e-mail systems, and other computing devices including but not limited to Personal Digital Assistants (PDAs), laptops, external hard drives, thumb drives or stand-alone PCs.

A. An "event" is any *possible* "breach" as breach is defined below.

SUBJECT: HIPAA AND CONFIDENTIALITY Event Report	*Chapter:* 19
	Section: 19.7
REFERENCES: Administrative Manual Policies: 11.6 Code of Conduct-Confidential Information; 11.11 Conflict of Interest; 19.7-CE or 19.7-O, Event Report Form; 24.2 Security Policies and Rules; and 24.7 Information Security Incident Reporting, and 42 U.S.C. 17921 of the HITECH Act; 45 CFR Parts 160 & 164; and §407.1500, RSMo	*Page:* 2 of 6
	Adopted: 7/23/10

B. **For covered entities within DHSS** subject to the Health Insurance Portability and Accountability Act of 1996 and its regulations (HIPAA):

1. A "breach" is ***any acquisition, access, use, or disclosure of protected health information in a manner not permitted by the HIPAA Privacy Rule which compromises the security or privacy of such information except as excluded under the rule***.

2. "Individual" shall mean the person who is the subject of protected health information.

3. "Protected health information" shall have the same meaning as provided by the HIPAA Privacy Rule.

4. "Unsecured protected health information" shall mean protected health information that is not "secure". Unencrypted electronic protected health information and papers records are not "secure."

C. **For non-covered entities within DHSS**, a "breach" is ***any unauthorized access to and unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information***.

1. The term "personal information" shall have the same meaning as defined in section 407.1500, RSMo, and as defined in paragraph IV.A.8 of Policy 19.2.

2. "Consumer" shall mean a resident of Missouri.

D. Examples of events include, but are not limited to: unauthorized access of information; unauthorized use of information; unauthorized disclosure of information; loss or theft of information or hardware containing information; and loss or theft of a laptop, USB drive, external memory device, etc.

SUBJECT: HIPAA AND CONFIDENTIALITY Event Report	*Chapter:* 19 Section: 19.7
REFERENCES: Administrative Manual Policies: 11.6 Code of Conduct-Confidential Information; 11.11 Conflict of Interest; 19.7-CE or 19.7-O, Event Report Form; 24.2 Security Policies and Rules; and 24.7 Information Security Incident Reporting, and 42 U.S.C. 17921 of the HITECH Act; 45 CFR Parts 160 & 164; and §407.1500, RSMo	*Page:* 3 of 6 *Adopted:* 7/23/10

III. POLICY:

This policy implements the DHSS Event Report Program requiring DHSS workforce to report any "event." The goal is to ensure prompt reporting of all events to the DHSS Privacy Officer, and to the Security Officer when electronic protected health information is involved, in order to minimize the possible impact of the event in terms of risk of harm to the individual/consumer or data loss, corruption, or system disruption; to prevent further events, attacks, or damages; address any legal issues, and assist DHSS to promptly notify individuals/consumers whose information is involved in a breach.

IV. PROCEDURES FOR EVENT REPORTS:

A. REPORTS MADE BY WORKFORCE MEMBERS:

1. If the event involves protected health information or personal information in non-electronic form only, workforce members must immediately:

   a. Make a report to the DHSS Privacy Officer by filling out an *Event Report* form and turning the *Event Report* form in to the DHSS Privacy Officer. DHSS HIPAA Covered Entities should use the *Event Report for Covered Entity* form, 19.7-CE, and Non-Covered Entities should use the *Event Report* for *Non-Covered Entity* form, 19.7-O.

   b. The *Event Report* form must be fully completed; however, the name and contact information for any individual/consumer whose protected health information or personal information was involved in the event shall be listed on Attachment 1 of the *Event Report* form.

2. If the event involves protected health information or personal information in **electronic form**, workforce members must immediately:

   a. Make a report to the DHSS Privacy Officer and the DHSS Security Officer following IV.A.1; and

   b. Follow all the additional requirements of Administrative Policy 24.7, *Information Security Incident Reporting*, in making the report to the DHSS Security Officer directly or through the DHSS Information Technology Services Division (ITSD) Help Desk.

B. REPORTS MADE BY BUSINESS ASSOCIATES OR CONTRACTORS:

1. Reports made by Business Associates of the covered entity portions of DHSS shall be made as set forth in the Business Associate Provisions of the contract in compliance with the HITECH Act, the Breach Notification Rule, and HIPAA.

2. Reports made by contractors of the portions of DHSS that are not covered entities shall be made as set forth in section 407.1500, RSMo or as specified by contract.

C. REPORTS MADE BY INDIVIDUAL(S) OR CONSUMER(S):

An individual, consumer, personal representative, or other person who wishes to report an event, shall be asked to submit a written report to the DHSS Privacy Officer, and to DHSS Security Officer if the event involves electronic protected health information or personal information, with specifics sufficient for investigation and the name and contact information for the person making the report. DHSS will not require an individual to waive the right to file a complaint provided by 45 CFR 160.306.

SUBJECT: HIPAA AND CONFIDENTIALITY Event Report	*Chapter:* 19
	Section: 19.7
REFERENCES: Administrative Manual Policies: 11.6 Code of Conduct-Confidential Information; 11.11 Conflict of Interest; 19.7-CE or 19.7-O, Event Report Form; 24.2 Security Policies and Rules; and 24.7 Information Security Incident Reporting, and 42 U.S.C. 17921 of the HITECH Act; 45 CFR Parts 160 & 164; and §407.1500, RSMo	*Page:* 5 of 6
	Adopted: 7/23/10

D. 19.7-CE or 19.7-O shall be processed by the DHSS team, including the DHSS Privacy Officer, and the DHSS Security Officer whenever electronic information is involved, in consultation with applicable DHSS workforce members to determine whether the event is a breach according to policy 19.8.

V. PROHIBITION OF RETALIATION:

No individual, consumer, employee, intern, trainee, volunteer, other workforce member, business associate, or contractor shall experience retaliation including intimidation, threats, coercion, discrimination and other retaliatory action, for filing an event report, cooperating with an investigation, or otherwise utilizing this policy. Witnesses are also protected from retaliation for participating in an investigation under this policy.

VI. ENFORCEMENT:

A. DHSS employees, interns, trainees, researchers, volunteers, or other workforce members who fail to comply with this policy are subject to disciplinary actions. These actions may include dismissal, depending on the severity of the offense, possible legal action, and other actions, including a report to the appropriate authorities.

B. DHSS contractors who fail to comply with this policy are subject to contract sanctions and other actions, including termination of the contract, a report to an appropriate authority, and possible legal action. Non-DHSS researchers who fail to comply with this policy are subject to sanctions and other actions, including a report to an appropriate authority and possible legal action.

C. Other individuals or entities may be referred to federal or state authorities for appropriate action.

SUBJECT: HIPAA AND CONFIDENTIALITY Event Report	*Chapter:* 19
	Section: 19.7
REFERENCES: Administrative Manual Policies: 11.6 Code of Conduct-Confidential Information; 11.11 Conflict of Interest; 19.7-CE or 19.7-O, Event Report Form; 24.2 Security Policies and Rules; and 24.7 Information Security Incident Reporting, and 42 U.S.C. 17921 of the HITECH Act; 45 CFR Parts 160 & 164; and §407.1500, RSMo	*Page:* 6 of 6
	Adopted: 7/23/10

Prepared By:

Approved By:

_____
Director
Information Technology Services Division

_____
Deputy Department Director

_____
Department Security Officer

_____
Department Privacy Officer

EVENT REPORT (FOR USE BY WORK FORCE OF A DHSS HIPAA COVERED ENTITY)

Instructions: The Department of Health and Senior Services prohibits unauthorized uses, disclosures, and breaches of protected health information and/or of personal information. If you believe that one of these events has occurred, complete the following and return to the Department Privacy Officer and Department Security Officer, Department of Health and Senior Services, 912 Wildwood, P.O. Box 570, Jefferson City, Missouri 65102.

REPORTER INFORMATION

_____ _____

NAME OF PERSON MAKING REPORT SIGNATURE DATE

_____

ORGANIZATIONAL UNIT AND WORK ADDRESS

_____

TELEPHONE NUMBER/FAX NUMBER

EVENT INFORMATION

1. DOES EVENT INVOLVE INFORMATION MAINTAINED BY OR ON BEHALF OF DHSS? YES __ NO __
2. DOES EVENT INVOLVE ELECTRONIC INFORMATION? YES __ NO __
   IF NO, PLEASE COMPLETE THIS FORM AND TURN IT IN TO THE DHSS PRIVACY OFFICER.
   IF YES, PLEASE FOLLOW THE PROCEDURES OF DHSS ADMINISTRATIVE POLICY 24.7, INFORMATION SECURITY INCIDENT REPORTING, AND COMPLETE THIS FORM AND TURN IT IN TO THE DHSS SECURITY OFFICER AND DHSS PRIVACY OFFICER.
   a. IF YES, WAS ELECTRONIC INFORMATION INVOLVED ENCRYPTED? YES __ NO __ UNK__
3. WAS THE EVENT CAUSED BY THE CONDUCT OF A DHSS EMPLOYEE, INTERN, TRAINEE OR VOLUNTEER? YES__ NO__ UNK__
   IF YES, IDENTIFY THE DHSS EMPLOYEE, INTERN, TRAINEE OR VOLUNTEER: _____
4. IDENTIFY DHSS DIVISION/SECTION/BUREAU/PROGRAM INVOLVED AND ITS CONTACT INFORMATION (For reports from State Public Health Laboratory: Attach copy of the SPHL Corrective Action Report and Result Report, skip remainder of Event Report, and turn all in to the Privacy Officer, and to the Security Officer *if* event involves electronic PHI.)
   _____
   _____
5. WAS THE EVENT CAUSED BY THE CONDUCT OF, OR OTHERWISE INVOLVE, ANOTHER ENTITY OR ITS EMPLOYEE(S)? YES__ NO__
   IF YES, IDENTIFY THAT ENTITY, ITS INVOLVEMENT, EMPLOYEE(S), CONTACT INFORMATION, AND THE RELATIONSHIP OF THE ENTITY WITH DHSS, such as BUSINESS ASSOCIATE, CONTRACTOR, OR OTHER RELATIONSHIP (for other relationship, please describe) :
   _____
   _____

6. DATE(S) OF EVENT(S): _____
7. IDENTIFY DATE(S) OF DISCOVERY and WHO DISCOVERED EVENT: _____
8. IDENTIFY DATE(S) OF REPORT TO DHSS and WHO REPORTED to DHSS: _____
9. DESCRIBE EVENT (PROVIDE SPECIFICS ABOUT HOW THE EVENT WAS DISCOVERED, HOW IT WAS BROUGHT TO YOUR ATTENTION, and WHAT HAPPENED WITHOUT IDENTIFYING THE INDIVIDUAL(S) WHOSE PROTECTED HEALTH INFORMATION WAS INVOLVED ON THIS FORM):

   _____

   _____

   (Attach additional pages as needed)
10. FILL OUT EVENT REPORT-ATTACHMENT 1 WITH NAME(S) AND CONTACT INFORMATION FOR INDIVIDUAL(S) WHOSE INFORMATION IS INVOLVED
11. TYPE(S) OF INFORMATION INVOLVED IN EVENT:

    YES __ NO __ FIRST NAME OF INDIVIDUAL YES __ NO __ FIRST INITIAL OF INDIVIDUAL

    YES __ NO __ LAST NAME OF INDIVIDUAL

    YES __ NO __ NAME OF INDIVIDUAL'S RELATIVE(S)

    YES __ NO __ NAME OF INDIVIDUAL'S EMPLOYER(S)

    YES __ NO __ NAME OF INDIVIDUAL'S HOUSEHOLD MEMBER(S)

    YES __ NO __ HOME STREET ADDRESS

    YES __ NO __ TOWN/CITY

    YES __ NO __ STATE

    YES __ NO __ ZIP CODE

    IF YES, FULL ZIP CODE __ PARTIAL ZIP CODE __

    IF PARTIAL, IDENTIFY HOW MANY AND WHICH DIGITS _ _ _ _ _ - _ _ _ _

    YES __ NO __ DATE OF BIRTH

    IF YES, __FULL DATE OF BIRTH __YEAR ONLY __OTHER

    YES __ NO __ DATE OF ADMISSION

    YES __ NO __ DATE(S) OF MEDICAL CARE/TREATMENT/VISIT/SERVICE

    YES __ NO __ DATE OF DISCHARGE

    YES __ NO __ DATE OF DEATH

    YES __ NO __ OTHER DATE(S) RELATED TO INDIVIDUAL

    YES __ NO __ TELEPHONE NUMBER(S)

    YES __ NO __ FAX NUMBER(S)

    YES __ NO __ EMAIL

    YES __ NO __ SOCIAL SECURITY NUMBER IF YES, FULL SS# __ OR PARTIAL SS# __

    IF PARTIAL SS#, PLEASE MARK (X) HOW MANY & WHICH DIGITS

    OF THE 9 DIGIT SEQUENCE: _ _ _-_ _ - _ _ _ _

    YES __ NO __ MEDICAL RECORD NUMBER(S)

    YES __ NO __ HEALTH PLAN BENEFICIARY NUMBER(S) (Any unique identifier used by insurer to identify the individual)

    YES __ NO __ DCN

    YES __ NO __ ACCOUNT NUMBER(S)

    YES __ NO __ CERTIFICATE/LICENSE NUMBER(S)

YES __ NO __ VEHICLE IDENTIFIER(S) OR SERIAL NUMBER(S), INCLUDING LICENSE PLATES
YES __ NO __ DEVICE IDENTIFIERS AND SERIAL NUMBERS
YES __ NO __ WEB UNIVERSAL RESOURCE LOCATORS (URLs)
YES __ NO __ INTERNET PROTOCOL (IP) ADDRESS NUMBER(S)
YES __ NO __ BIOMETRIC IDENTIFIERS, INCL. VOICE/FINGER PRINTS
YES __ NO __ FULL FACE PHOTO AND ANY COMPARABLE IMAGES
YES __ NO __ ANY OTHER UNIQUE IDENTIFYING NUMBER
IF YES, WHAT TYPE OF NUMBER _____
IF YES, IS IT A NUMBER CREATED OR COLLECTED BY A GOVERNMENT AGENCY?
YES __ NO __ DISABILITY CODE
YES __ NO __ MEDICAL INFORMATION
YES __ NO __ FINANCIAL ACCOUNT NUMBER, CREDIT CARD NUMBER, OR DEBIT ACCOUNT NUMBER IN COMBINATION WITH ANY SECURITY OR ACCESS CODE OR PASSWORD THAT WOULD PERMIT ACCESS TO AN INDIVIDUAL'S FINANCIAL ACCOUNT
YES __ NO __ UNIQUE ELECTRONIC IDENTIFIER OR ROUTING CODE, IN COMBINATION WITH ANY REQUIRED SECURITY OR ACCESS CODE OR PASSWORD THAT WOULD PERMIT ACCESS TO AN INDIVIDUAL'S FINANCIAL ACCOUNT

12. IS ADDRESS UNAVAILABLE FOR:
    a. AT LEAST ONE, BUT LESS THAN TEN (10) INDIVIDUALS LISTED IN ATTACHMENT 1? YES __ NO__
    b. TEN (10) OR MORE OF INDIVIDUALS LISTED IN ATTACHMENT 1? YES __ NO __
13. ARE THERE FIVE HUNDRED (500) OR MORE INDIVIDUALS WHOSE INFORMATION IS INVOLVED? YES __ NO __
14. IS LAW ENFORCEMENT AWARE OF THE SITUATION? YES __ NO __ UNK __
    IF YES, IDENTIFY LAW ENFORCEMENT AGENCY AND ITS CONTACT INFORMATION
    _____
    _____
    - IS YES, DID LAW ENFORCEMENT REQUEST A DELAY OF NOTIFICATION TO INDIVIDUAL(S) WHO MAY NEED TO BE NOTIFIED? YES __ NO __ UNK __
    - IF YES, WAS REQUEST WRITTEN OR VERBAL? WRITTEN __ VERBAL __
    - IF WRITTEN, ATTACH COPY OF THE WRITTEN REQUEST LAW ENFORCEMENT REQUEST.
    - IF VERBAL, ATTACH COPY OF YOUR DOCUMENTATION OF THE VERBAL REQUEST.
15. IS THE INFORMATION AT RISK OF IMMINENT MISUSE? YES __ NO __ UNK __
    IF YES, EXPLAIN: _____
16. HAS CORRECTIVE ACTION BEEN TAKEN TO END THE EVENT? YES __ NO __ UNK __
    IF YES, WHAT ACTION HAS BEEN TAKEN? _____
    IF NO, WHAT ACTION IS RECOMMENDED? _____
17. RECOMMENDED STEPS INDIVIDUALS SHOULD TAKE TO PROTECT THEMSELVES FROM RISK OF HARM FROM THE EVENT: _____
    _____

19.7- CE Attachment 1

ATTACHMENT 1

NAME	ADDRESS	TELEPHONE NUMBER	EMAIL(if individual has specified a preference for contact by email)
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Add additional pages as needed to list all individuals/consumers.

EVENT REPORT (FOR USE BY WORKFORCE OF A DHSS NON-COVERED ENTITY)

Instructions: The Department of Health and Senior Services prohibits unauthorized uses or disclosures and breaches of protected health information and/or of personal information. If you believe that one of these events has occurred, complete the following and return to the Department Privacy Officer, and to Department Security Officer if electronic information is involved, Department of Health and Senior Services, 912 Wildwood, P.O. Box 570, Jefferson City, Missouri 65102.

REPORTER INFORMATION

_____ _____

NAME OF PERSON MAKING REPORT SIGNATURE DATE

_____

ORGANIZATIONAL UNIT AND WORK ADDRESS

_____

TELEPHONE NUMBER/FAX NUMBER

EVENT INFORMATION

1. DOES EVENT INVOLVE INFORMATION MAINTAINED BY OR ON BEHALF OF DHSS? YES __ NO __
2. DOES EVENT INVOLVE ELECTRONIC INFORMATION? YES __ NO __
   IF NO, PLEASE COMPLETE THIS FORM AND TURN IT IN TO THE DHSS PRIVACY OFFICER.
   IF YES, PLEASE FOLLOW THE PROCEDURES OF DHSS ADMINISTRATIVE POLICY 24.7, INFORMATION SECURITY INCIDENT REPORTING, AND COMPLETE THIS FORM AND TURN IT IN TO THE DHSS SECURITY OFFICER AND DHSS PRIVACY OFFICER.
   a. IF YES, WAS ELECTRONIC INFORMATION INVOLVED ENCRYPTED? YES __ NO __ UNK__
3. WAS THE EVENT CAUSED BY THE CONDUCT OF A DHSS EMPLOYEE, INTERN, TRAINEE OR VOLUNTEER? YES__ NO__ UNK__
   IF YES, IDENTIFY THE DHSS EMPLOYEE, INTERN, TRAINEE OR VOLUNTEER: _____
4. IDENTIFY DHSS DIVISION/SECTION/BUREAU/PROGRAM INVOLVED AND ITS CONTACT INFORMATION: _____
   _____
5. WAS THE EVENT CAUSED BY THE CONDUCT OF, OR OTHERWISE INVOLVE, ANOTHER ENTITY OR ITS EMPLOYEE(S)? YES__ NO__
   IF YES, IDENTIFY THAT ENTITY, ITS INVOLVEMENT, EMPLOYEE(S), CONTACT INFORMATION, AND THE RELATIONSHIP OF THE ENTITY WITH DHSS, such as CONTRACTOR OR OTHER RELATIONSHIP (for other relationship, please describe) : _____
   _____
6. DATE(S) OF EVENT(S): _____
7. IDENTIFY DATE(S) OF DISCOVERY and WHO DISCOVERED EVENT: _____
8. IDENTIFY DATE(S) OF REPORT TO DHSS and WHO REPORTED to DHSS: _____

9. DESCRIBE EVENT (PROVIDE SPECIFICS ABOUT HOW THE EVENT WAS DISCOVERED, HOW IT WAS BROUGHT TO YOUR ATTENTION, and WHAT HAPPENED WITHOUT IDENTIFYING THE CONSUMER(S) WHOSE PERSONAL INFORMATION WAS INVOLVED ON THIS FORM):

   _____

   _____

   (Attach additional pages as needed)
10. FILL OUT **EVENT REPORT**-**ATTACHMENT 1** WITH NAMES AND CONTACT INFORMATION FOR CONSUMER(S) WHOSE INFORMATION IS INVOLVED.
11. TYPE(S) OF INFORMATION INVOLVED IN EVENT:

    YES __ NO __ FIRST NAME OF INDIVIDUAL/CONSUMER

    YES __ NO __ FIRST INITIAL OF INDIVIDUAL/CONSUMER

    YES __ NO __ LAST NAME OF INDIVIDUAL/CONSUMER

    YES __ NO __ SOCIAL SECURITY NUMBER

    IF YES, FULL SS# __ OR PARTIAL SS# __

    IF PARTIAL SS#, PLEASE MARK (X) HOW MANY & WHICH DIGITS OF the 9 DIGIT SEQUENCE: _ _ _-_ _ - _ _ _ _

    YES __ NO __ DRIVERS LICENSE NUMBER

    YES __ NO __ ANY OTHER UNIQUE IDENTIFYING NUMBER CREATED OR COLLECTED BY A GOVERNMENT AGENCY

    IF YES, WHAT TYPE OF NUMBER _____

    YES __ NO __ FINANCIAL ACCOUNT NUMBER, CREDIT CARD NUMBER, OR DEBIT ACCOUNT NUMBER IN COMBINATION WITH ANY SECURITY OR ACCESS CODE OR PASSWORD THAT WOULD PERMIT ACCESS TO AN INDIVIDUAL'S FINANCIAL ACCOUNT

    YES __ NO __ UNIQUE ELECTRONIC IDENTIFIER OR ROUTING CODE, IN COMBINATION WITH ANY REQUIRED SECURITY OR ACCESS CODE OR PASSWORD THAT WOULD PERMIT ACCESS TO AN INDIVIDUAL'S FINANCIAL ACCOUNT

    YES __ NO __ MEDICAL INFORMATION (ANY INFORMATION REGARDING A CONSUMER'S MEDICAL HISTORY, MENTAL OR PHYSICAL CONDITION, OR MEDICAL TREATMENT OR DIAGNOSIS BY A HEALTH CARE PROFESSIONAL)

    YES __ NO __ HEALTH INSURANCE INFORMATION (AN INDIVIDUAL'S HEALTH INSURANCE POLICY NUMBER OR SUBSCRIBER IDENTIFICATION NUMBER, ANY UNIQUE IDENTIFIER USED BY A HEALTH INSURER TO IDENTIFY THE INDIVIDUAL)

12. IS ADDRESS UNAVAILABLE FOR:
    a. AT LEAST ONE, BUT LESS THAN TEN (10) INDIVIDUALS LISTED IN ATTACHMENT 1? YES __ NO__
    b. TEN (10) OR MORE OF INDIVIDUALS LISTED IN ATTACHMENT 1? YES __ NO __
13. ARE THERE FIVE HUNDRED (500) OR MORE CONSUMERS WHOSE INFORMATION IS INVOLVED? YES __ NO __
14. ARE THERE ONE THOUSAND (1000) OR MORE CONSUMERS WHOSE INFORMATION IS INVOLVED? YES __ NO __
15. IS LAW ENFORCEMENT AWARE OF THE SITUATION? YES __ NO __ UNK __

IF YES, IDENTIFY LAW ENFORCEMENT AGENCY AND ITS CONTACT INFORMATION

_____

_____

IS YES, DID LAW ENFORCEMENT REQUEST A DELAY OF NOTIFICATION TO CONSUMER(S) WHO MAY NEED TO BE NOTIFIED? YES __ NO __ UNK __

IF YES, WAS REQUEST WRITTEN OR VERBAL? WRITTEN __ VERBAL __

IF WRITTEN, ATTACH COPY OF THE WRITTEN REQUEST.

IF VERBAL, ATTACH COPY OF YOUR DOCUMENTATION OF THE VERBAL REQUEST.

16. IS THE INFORMATION AT RISK OF IMMINENT MISUSE? YES __ NO __ UNK __
    IF YES, EXPLAIN: _____
17. HAS CORRECTIVE ACTION BEEN TAKEN TO END THE EVENT? YES __ NO __ UNK __
    IF YES, WHAT ACTION HAS BEEN TAKEN? _____
18. RECOMMENDED STEPS INDIVIDUALS SHOULD TAKE TO PROTECT THEMSELVES FROM RISK OF HARM FROM THE EVENT: _____

    _____

19.7- O Attachment 1

ATTACHMENT 1

NAME	ADDRESS	TELEPHONE NUMBER	EMAIL(if individual has specified a preference for contact by email)
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Add additional pages as needed to list all individuals/consumers.

SUBJECT: HIPAA AND CONFIDENTIALITY Breach Notification	*Chapter:* 19 *Section:* 19.8
REFERENCES: Administrative Manual Policies: 11.6 Code of Conduct-Confidential Information, 11.11 Conflict of Interest, 19.7 Event Report, 24.2 Security Policies and Rules, 24.7 Information Security Incident Reporting, and 42 U.S.C. 17921 of the HITECH Act, 45 CFR Parts 160 & 164, §407.1500, RSMo	*Page:* 1 of 7 *Adopted:* 7/23/10

BREACH NOTIFICATION

I. PURPOSE:

This policy establishes the Department of Health and Senior Services (DHSS) Breach Notification process and identifies the procedures, roles and responsibilities needed for its implementation. The purpose is to establish a process for assessing reported events to determine whether an event is a breach requiring notification of an individual or consumer in order to provide for prompt Breach Notification to individuals whose protected health information or personal information was involved in a breach as defined in Policy 19.7.

II. SCOPE:

This policy applies to all DHSS workforce members, including all employees, interns, trainees, researchers, and volunteers who report or should report an event as defined in Policy 19.7 and to the compliance team, comprised of the DHSS Privacy Officer, Security Officer and others depending on the circumstances, who will gather relevant information and assess the circumstances and facts to determine if Breach Notification is required and whether other action should be recommended to the Office of Human Resources and DHSS management. This policy also applies to contractors.

III. POLICY:

DHSS will implement a Breach Notification Program to minimize the possible impact of an event in terms of harm to the individual/consumer, prevent breaches, address any legal issues, and to ensure prompt notification of individuals/consumers whose protected health information or personal information is at risk of harm due to a breach.

IV. PROCEDURE FOR EVENT REVIEW/RISK ASSESSMENT:

A. Any workforce member with knowledge of an event shall cooperate fully with the investigation.

B. A contractor or researcher with knowledge of an event shall cooperate fully with the investigation. A contractor or researcher whose actions or omissions result in a breach may be required to cover the costs of any Breach Notifications required under this policy.

C. The Privacy Officer and/or Security Officer shall review form 19.7-CE or 19.7-O, the Event Report, and obtain any additional information required to determine if the event is a breach with the assistance of the DHSS workforce, DHSS Office of Human Resources (HR), and Information Technology Services Division (ITSD).

D. The Privacy Officer and/or Security Officer shall use form 19.8A Event Review/Risk Assessment to review and assess a reported event to determine whether the event is a breach.

E. The Privacy Officer and/or Security Officer shall use form 19.8B Action Report to document:

1. Whether the event is a breach requiring notification;

2. Whether, and what, measures should be recommended to the individual(s)/consumer(s) if the event is a breach; and

3. Whether, and what, measures should be undertaken by DHSS to correct and/or mitigate the breach if the event is found to be a breach, including but not limited to employment sanctions, contract actions and/or protections for the individuals. The recommendation shall consider the requirement of 45 CFR 164.530(f) that

DHSS mitigate to the extent practicable any harmful effect known by DHSS resulting from a use or disclosure in violation of its policies or the Privacy Rule.

F. The Privacy Officer and Security Officer will refer:

1. Any recommendation for employment sanctions to applicable programmatic staff and Human Resources for further action.

2. Any recommendation for contract sanctions/actions to applicable programmatic staff and the DHSS Office of Administration for further action.

G. If it is determined that a breach requiring breach notification has occurred, DHSS will provide each individual/consumer whose information was involved with Breach Notification as set out below.

V. PROCEDURE FOR BREACH NOTIFICATION:

A. STANDARD: DHSS shall provide Breach Notification to an individual whose protected health information or personal information is compromised by the breach of his/her protected health information or personal information.

B. MANNER AND FORMAT: The Breach Notification shall be provided in WRITING in the following manner and format:

1. TO WHOM: TO THE INDIVIDUAL, or if the individual is deceased to the individual's next of kin or personal representative. In addition, for a breach involving more than five hundred (500) individuals, the DHSS Office of Public Information shall also provide notice to prominent media serving the state;

2. HOW: BY U.S. FIRST CLASS MAIL, or if the individual agrees to electronic notice, then notification may be by email. If there is possible imminent misuse of protected health information, then additional notice by telephone or other means is also required;

3. WHEN: WITHOUT UNREASONABLE DELAY, no later than sixty (60) days after discovery of the breach by DHSS (if a breach determination cannot be made prior to 60 days, notification shall be provided).

   However, if law enforcement requests a delay required for law enforcement purposes, breach notification may be delayed for the period of time specified in the written law enforcement request. Breach notification may not be delayed for more than thirty (30) days if the law enforcement request is not made in writing.

4. WHERE: TO THE INDIVIDUAL'S LAST KNOWN ADDRESS, or by substitute notice if the last known address is insufficient or out of date. If the address is unknown or out of date for less than ten (10) individuals, for those specific individuals substitute notification shall be made by a telephone call or face-to-face communication to the individual and documented.

   If the address is unknown or out of date for more than ten (10) individuals, for those specific individuals substitute notification shall be made by an Office of Public Information posting on the DHSS website (or in print or broadcast media) with the toll-free number 1-800-392-0272 provided for individuals to call to determine if their information was breached.

   Substitute notice is not required for a deceased individual if the address of the next of kin is unknown or out of date.

NOTE: See 19.8C: Breach Notification Flow Chart: The Breach notification flow chart illustrates the steps and process required for notification.

C. CONTENT OF BREACH NOTIFICATION

The Breach Notification shall contain:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

2. A description of the types of unsecured Protected Health Information or Personal Information involved;

3. Any steps individuals should take to protect themselves from potential harm resulting from the breach;

4. A brief description of what DHSS (or its contractor) is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

5. Contact procedures for individuals to ask questions or learn additional information, including the DHSS mailing address Missouri Department of Health and Senior Services, P.O. Box 570, Jefferson City, MO 65102: Attention: Privacy Officer and email address Privacy@dhss.mo.gov. For events involving ten (10) or more individuals, individuals will be provided the toll-free telephone number 1-800-392-0272 instead of the email address.

VI. DOCUMENTATION:

A. Any event determined to be a breach involving one of the DHSS HIPAA covered entities or its Business Associate shall be documented as a HIPAA breach; and included in an annual breach report to the US Department of Health and Human Services (HHS) of breaches by the covered entities of DHSS and/or their business associates, except that:

1. Breaches involving five hundred (500) or more individuals shall be reported to HHS concurrently with the Breach Notification to the individual.

2. The Event Report, Event Review/Risk Assessment, Action Report, and any other applicable documents shall be maintained for six (6) years, along with a copy of the Breach Notification.

B. Any event determined to be a breach involving a DHSS non-covered entity or its contractor:

1. Shall be documented as a section 407.1500, RSMo, breach.

2. The Event Report, Event Review/Risk Assessment, Action Report, and any other applicable documents shall be maintained for six (6) years, along with a copy of the Breach Notification.

C. Any event determined not to be a breach shall be documented. The Event Report, Event Review/Risk Assessment, Action Report, and any other applicable documents must be maintained for six (6) years.

VII. ENFORCEMENT:

A. DHSS employees, interns, trainees, researchers, volunteers, or other workforce members whose actions or omissions result in a breach or who fail to comply with this policy are subject to disciplinary actions, up to and including dismissal; possible legal action; and other actions, including a report to the appropriate authorities.

B. DHSS contractors whose actions or omissions result in a breach or who fail to comply with this policy are subject to contract sanctions and other actions, including termination of the contract, a report to an appropriate authority, and possible legal action.

SUBJECT: HIPAA AND CONFIDENTIALITY Breach Notification	*Chapter:* 19
	Section: 19.8
REFERENCES: Administrative Manual Policies: 11.6 Code of Conduct-Confidential Information, 11.11 Conflict of Interest, 19.7 Event Report, 24.2 Security Policies and Rules, 24.7 Information Security Incident Reporting, and 42 U.S.C. 17921 of the HITECH Act, 45 CFR Parts 160 & 164, §407.1500, RSMo	*Page:* 7 of 7
	Adopted: 7/23/10

C. Non-DHSS researchers who fail to comply with this policy are subject to sanctions and other actions, including a report to an appropriate authority and possible legal action.

D. Other individuals or entities may be referred to federal or state authorities for appropriate action.

Prepared By:

_____

Director
Information Technology Services Division

_____

Department Privacy Officer

Approved By:

_____

Deputy Department Director

EVENT REVIEW/RISK ASSESSMENT: Is the event a breach?

Date discovered	
Date reported:	
Date of determination	
Investigation Team	

T/F/NA		
	1	**Unauthorized access, acquisition, use, disclosure of protected health information (covered entity) or personal information (non-covered entity).**
	2	**The information was known to be de-identified.**
		If True, the event was not a breach.
	3	**The information was unusable, unreadable or indecipherable (secure).**
		If True, the event does not *require* Breach Notification unless the key was also disclosed.
	4	**The access, use or disclosure of the information does not pose a significant risk of financial, reputational or other harm to the individual(s). Explain:** _____ _____ _____ ***If it does pose a risk, describe the risk:**
		If True, the event was not a breach.
	5	**An incident of access or use:** ☐ **Was unintentional** ☐ **Was made in good faith by an authorized person of the CE or BA** ☐ **Occurred within the scope of that person's authority** ☐ **Was not further used or disclosed in violation of the Privacy Rule** ***In order for statement to be true, every sub-statement must be true.***
	6	**An incident of disclosure:** ☐ **Was inadvertent** ☐ **Was made in good faith by an authorized person of a CE or BA** ☐ **Was made to another authorized person at the same CE or BA** ☐ **Was not further used or disclosed in violation of the Privacy Rule** ***In order for statement to be true, every sub-statement must be true.***
	7	**An incident of disclosure was made to an unauthorized person but the CE or BA has a good faith belief that the unauthorized recipient would not reasonably have been able to retain the information.**
	8	**The information was known to be a Limited Data Set that also excluded zip code and date of birth.**
		If 5, 6, 7, or 8 True, the event was not a breach.

DETERMINATION

	The event is a breach requiring notification
	The event is NOT a breach.

Completed by:	

CE= covered entity BA= business associate

ACTION REPORT FOR EVENT REPORT # _____

1. DATE OF INCIDENT:
2. DATE OF DISCOVERY:
3. DISCOVERY BY:
4. DATE OF REPORT TO DHSS: _____ Is this the date of DHSS DISCOVERY? Y/N
5. NOTIFICATION WITHIN 60 DAYS of DHSS DISCOVERY SO NOTIFICATION WOULD BE REQUIRED BY: _____
6. RISK ASSESSMENT: None__ Some__ High__
7. RISK OF IMMINENT MISUSE: (PROMPT NOTIFICATION REQUIRED) _____
8. CONDUCT OF DHSS, BAA, OTHER CONTRACTOR, OR OTHER ENTITY:
9. COVERED ENTITY OR NON-COVERED ENTITY:
10. PHI OR PI:
11. ELECTRONIC OR NON-ELECTRONIC:
12. ENCRYPTED OR NOT ENCRYPTED (SECURE/NOT SECURE):
13. LESS THAN 10 UNKNOWN ADDRESS:
14. 10 OR MORE WITH UNKNOWN ADDRESS:
15. LESS THAN 10 WITH RETURNED NOTIFICATION DUE TO OUT OF DATE ADDRESS:
16. 10 OR MORE WITH RETURNED NOTIFICATION DUE TO OUT OF DATE ADDRESS:
17. 500 OR MORE INDIVIDUALS INVOLVED:
18. LAW ENFORCEMENT REQUEST FOR DELAY OF NOTIFICATION (WRITTEN DOCUMENTATION OF REQUEST REQUIRED FOR DELAY OF GREATER THAN 30 DAYS):
19. STEPS TAKEN TO CORRECT: _
20. IS REMEDIATION RECOMMENDED? NO __ YES __
21. IF YES, WHAT REMEDIATION? _____
22. ACTION REQUIRED:

__ a. Document as Breach and make Notification:

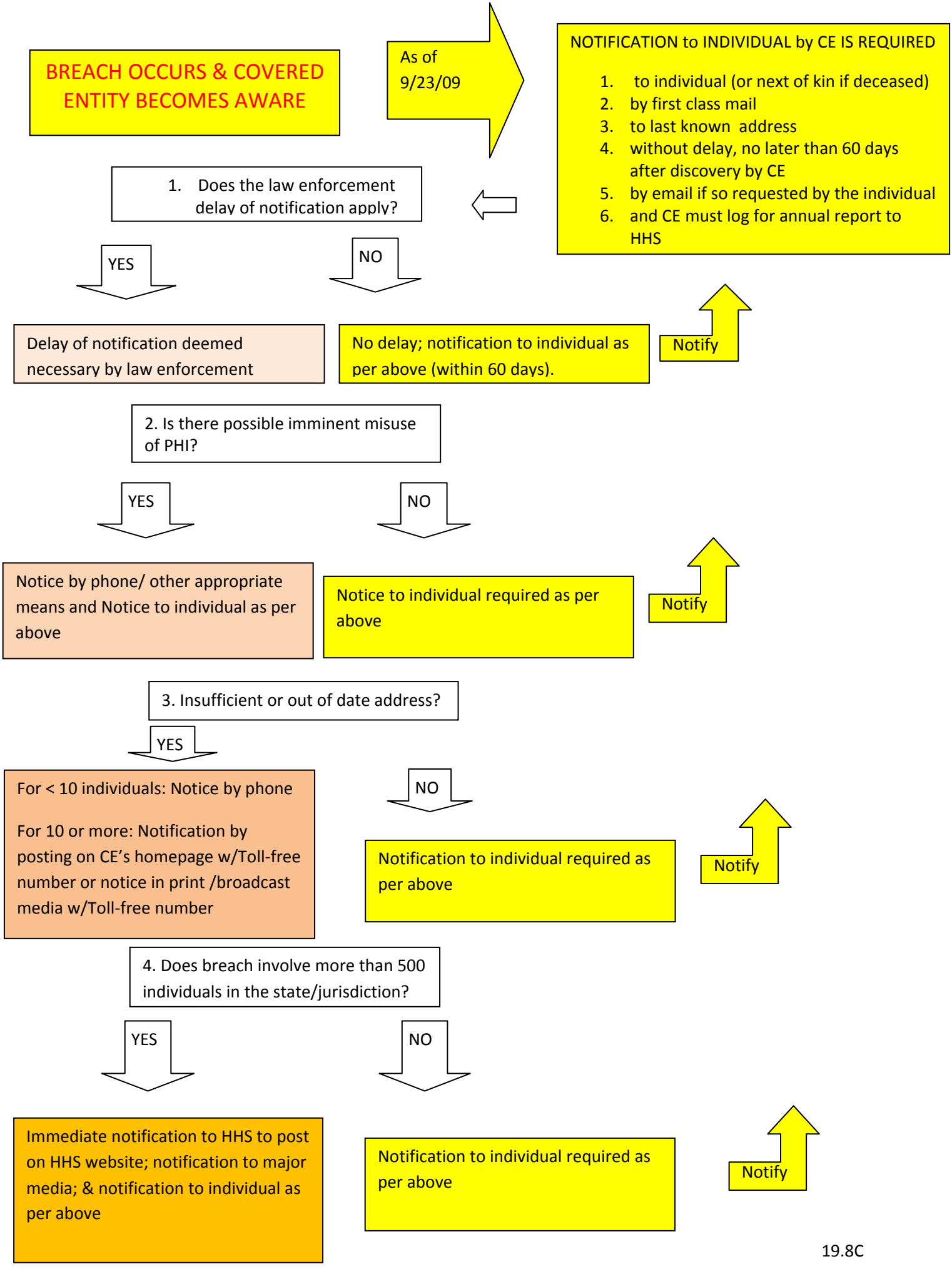
i. To:
   a. __The individual(s)_____;
      or
   b. __To another entity: _____

ii. TO HHS by:
   a. __Logging for annual report. (http://transparency.cit.nih.gov/breach/index.cfm);
      or
   b. __Making a report to HHS simultaneously with notification to the individual(s). http://transparency.cit.nih.gov/breach/index.cfm

__ b. Document as Non-Breach and maintain documentation.

i. Was another agency notified: NO__ YES__
   a. If yes, identify the other agency notified: _____.

ACTION REPORT COMPLETED BY: _____SIGNATURE_____DATE_____


BREACH OCCURS & COVERED ENTITY BECOMES AWARE
As of 9/23/09
NOTIFICATION to INDIVIDUAL by CE IS REQUIRED
1. to individual (or next of kin if deceased)
2. by first class mail
3. to last known address
4. without delay, no later than 60 days after discovery by CE
5. by email if so requested by the individual
6. and CE must log for annual report to HHS
1. Does the law enforcement delay of notification apply?
YES
NO
Delay of notification deemed necessary by law enforcement
No delay; notification to individual as per above (within 60 days).
Notify
2. Is there possible imminent misuse of PHI?
YES
NO
Notice by phone/ other appropriate means and Notice to individual as per above
Notice to individual required as per above
Notify
3. Insufficient or out of date address?
YES
For < 10 individuals: Notice by phone
For 10 or more: Notification by posting on CE's homepage w/Toll-free number or notice in print /broadcast media w/Toll-free number
NO
Notification to individual required as per above
Notify
4. Does breach involve more than 500 individuals in the state/jurisdiction?
YES
NO
Immediate notification to HHS to post on HHS website; notification to major media; & notification to individual as per above
Notification to individual required as per above
Notify